CLAIMS

1. A method for managing authentication information for a user, the method comprising the steps of:

receiving a master digital key from the user;

obtaining authentication of the user based on the master digital key;

receiving from the user a selection of one identity from among a plurality of identities that are stored for the user; and

providing authentication information for the user into an application or web page based on the one identity selected by the user.

2. The method of claim 1, wherein the providing step comprises the sub-steps of:

recognizing a web page for which authentication information is stored; and

automatically filling the authentication information for the user into appropriate elements of the web page.

3. The method of claim 1, wherein the providing step comprises the sub-steps of:

providing the user with a list of web pages for which authentication information is stored;

receiving from the user a selection of one web page from the list of web pages; and

automatically opening the one web page selected by the user, and filling the authentication information for the user into appropriate elements of the web page.

4. The method of claim 1, further comprising the steps of:

receiving an address of a web page from the user;

downloading and analyzing the web page in order to determine what authentication information is required by the web page;

presenting the user with a list of the authentication information that is required by the web page; and

storing authentication information entered by the user in response to the list.

5. The method of claim 1, further comprising the steps of:

recognizing a web page that requires authentication information; and

storing authentication information entered into the web page by the user.

6. The method of claim 1, wherein the authentication information provided for the user includes a complete state of the web page, including states of any checkboxes and radio buttons.

7. The method of claim 1, wherein two of the identities store different authentication information for the user for the same application or web page.

8. The method of claim 1, wherein in the step of providing authentication information for the user, the authentication information for the user is provided to a web page on behalf of a third party application without allowing the third party application access to the authentication information.

9. A computer program product for creating a new annotation for a data source, the computer program product comprising:

a storage medium readable by a processing circuit and storing instructions for execution by the processing circuit for performing a method comprising the steps of:

receiving a master digital key from the user;

obtaining authentication of the user based on the master digital key;

receiving from the user a selection of one identity from among a plurality of identities that are stored for the user; and

providing authentication information for the user into an application or web page based on the one identity selected by the user.

10. The computer program product of claim 9, wherein the providing step comprises the sub-steps of:

recognizing a web page for which authentication information is stored; and

automatically filling the authentication information for the user into appropriate elements of the web page.

11. The computer program product of claim 9, wherein the providing step comprises the sub-steps of:

providing the user with a list of web pages for which authentication information is stored;

receiving from the user a selection of one web page from the list of web pages; and

automatically opening the one web page selected by the user, and filling the authentication information for the user into appropriate elements of the web page.

12. The computer program product of claim 9, wherein the method further comprises the steps of:

receiving an address of a web page from the user;

downloading and analyzing the web page in order to determine what authentication information is required by the web page;

presenting the user with a list of the authentication information that is required by the web page; and

storing authentication information entered by the user in response to the list.

13. The computer program product of claim 9, wherein the method further comprises the steps of:

recognizing a web page that requires authentication information; and

storing authentication information entered into the web page by the user.

14. The computer program product of claim 9, wherein two of the identities store different authentication information for the user for the same application or web page.

15. A system for managing authentication information for a user, the system comprising:

a first interface receiving a master digital key from the user;

a second interface receiving from the user a selection of one identity from among a plurality of identities that are stored for the user; and

an ID manager providing authentication information for the user into an application or web page based on the one identity selected by the user,

wherein authentication of the user is obtained based on the master digital key.

16. The system of claim 15, wherein the ID manager recognizes a web page for which authentication information is stored, and automatically fills the authentication information for the user into appropriate elements of the web page.

17. The system of claim 15, wherein the ID manager provides the user with a list of web pages for which authentication information is stored, receives from the user a selection of one web page from the list of web pages, automatically opens the one web page selected by the user, and fills the authentication information for the user into appropriate elements of the web page.

18. The system of claim 15, further comprising:

a third interface receiving an address of a web page from the user,

wherein the ID manager analyzes the web page in order to determine what authentication information is required by the web page and presents the user with a list of the authentication information that is required by the web page, and

the system further comprises an ID store that stores authentication information entered by the user in response to the list.

19. The system of claim 15,

wherein the ID manager recognizes a web page that requires authentication information, and

the system further comprises an ID store that stores authentication information entered into the web page by the user.

20. The system of claim 15, wherein the ID manager provides the authentication information for the user to a web page on behalf of a third party application without allowing the third party application access to the authentication information.